



samphire

Quarterly Report

Malicious Risks,  
In Depth: United  
States of America





# Contents

4	Foreword
5	Definitions Relating to this Report
8	Malicious Threats in the US Today
12	Emerging Trends
16	Existing Market Mitigation Strategies
17	Conclusion
18	About Samphire Advisory



## Foreword

Samphire Quarterly Insight Reports provide analysis on the developing malicious risk landscape globally. The US is of course a core element of this landscape with dynamics that have the potential to influence globally.

For this reason, this Quarterly Report will consider the existing and developing malicious risk environment in the US. An environment that has been knocked from pillar to post in the last few years with polarizing elections; rioting; extremism; and, of course, violence due to the proliferation of firearms.

We will seek to establish what threats have the potential to impact the US now, as well as identify emerging factors which could change the threat picture in the future. Finally, we assess current risk transfer strategies to offer an opinion on whether the protection they intend to offer is sufficiently responsive for the evolving risk environment.

I hope that you enjoy the report.

**Charlie Hanbury**  
**Chief Executive Officer**  
**Samphire Risk**



# Definitions Relating to this Report

Given the focus in this report on the malicious risk landscape in the US, the peril definitions used are in line with either the US government, US law enforcement, or leading US academic institutions. Where US-specific definitions are not available, we have used insurance industry defined terms. The following terms and perils will be defined as follows throughout this report:

<b>Terrorism</b>	The unlawful use of force or violence against persons or property to intimidate or coerce a government or civilian population in furtherance of political or social objectives.
<b>Sabotage</b>	The actual or attempted damage, disruption, or subversion of the target entity's operations. Carried out by persons who are solely and directly targeting the insured's physical property for the purpose of effecting unfavorable publicity, delays in production, damage to physical property, the destruction of working relationships, or the harming of the insured's employees or customers.
<b>Political violence (PV)</b>	Force or violence used with a political motivation to achieve a political goal, to assert political power over another group, or to disseminate a political message to an outside audience. Force or violence includes any form of direct physical harm or the threat thereof to persons or property as well as intimidation in which such threats are implicit.
<b>Strikes, riots and civil commotion (SRCC)</b>	<p>A strike means a work stoppage to enforce demands made on an employer or to protest against an act or condition.</p> <p>A riot means a violent disturbance by a group of persons assembled together for a common purpose which threatens the public peace.</p> <p>Civil commotion means a substantial violent uprising by a large number of persons assembled together and acting with common purpose or intent.</p>



# Definitions Relating to this Report

## Why are these definitions important?

Historically, the insurance market has offered cover for these perils as stand-alone products (terrorism cover, sabotage cover, SRCC cover, etc.) and these have focused on transferring the risk of specific, identified, and clearly defined losses (property damage, business interruption, and liability) for example:

A terrorism policy typically covered property damage and business interruption but excluded war, military action, invasion, civil war, rebellion, and insurrection.

SRCC insurance provided cover for loss or damage to property and people caused directly by "strikers, locked-out workers, people involved in work related unrest and riots of various kinds, or by a riot involving a large number of people whose collective action causes damage to people or property".<sup>1</sup>

In the 1980s (when the global malicious risk environment was relatively stable) and the 1990s (when the implications of recent geostrategic change had yet to be fully exposed or understood) this cover suited the market and broadly speaking, the insured. However, by the early 2000s the malicious risk landscape had undergone profound change; most especially of course following the 9/11 attacks.

With exposure increasing; existing exclusions and sub-limits in place; and with access to policies continuing to be constrained by narrowly defined triggers, the cover offered often fell short of what was required by insureds. The relevance of existing products also began to be questioned by carriers.

As a result, while carriers and brokers continue to offer stand-alone insurance for individual risks, the market has now long recognized that there is also a requirement for blended solutions which provide cover for a range of risks under a single policy.

While legacy exposure definitions for perils such as terrorism, sabotage, and SRCC continue to be used, these are now frequently employed in combination.

To help explain the broader range of cover these new products now provide, it is worth considering the definitions below:

**Insured Triggers:** political violence and terrorism insurance protects against physical damage and business interruption losses caused by: terrorism; riots, strikes and civil unrest; insurrection, revolution and rebellion; political violence, including war and civil war; looting and pillaging; contingent business interruption; and ongoing threats;<sup>2</sup> and

**Insured Losses:** terrorism and political violence insurance protects organizations against impacts of terrorism and political violence, including: property damage to insured assets; business interruption; contingent time risks (including denial of access, loss of attraction, customers and suppliers, and others on request); third-party terrorism liability; cyber terrorism; malicious attack/active assailant; event cancellation; and terrorism/PV reinsurance.<sup>3</sup>

## The importance of a blended view

With many carriers now offering cover for political violence including losses triggered by terrorism, sabotage, SRCC, active assailant, active assailant, and war, it is no longer correct to analyze exposure in silos. Instead, a blended view is required, one that incorporates a fused threat that spans a spectrum of perils. Exposure management that considers terrorism, through sabotage, active assailant and active shooter, to war and SRCC is now more likely to capture the contemporary and developing threat landscape.

However, because each of these perils is also covered individually, there is merit in exploring each in turn to establish the scale and scope of the risk they pose. Firstly, this is to identify the possibility and likelihood of one or more coalescing to see if they could present a peril greater than the insured sum of their parts.

Secondly, this allows us to consider if existing market solutions offer the optimum means of delivering the cover most likely to be required by the insured if they are to protect their people, their assets, and their bottom line.

Exposure management that considers terrorism, through sabotage, active assailant and active shooter, to war and SRCC is now more likely to capture the contemporary and developing threat landscape.



# Malicious Threats in the US Today

## Terrorism

### Domestic terrorism

Over the next couple of years, the threat of violence from extremists radicalized in the United States will remain high but largely unchanged from the threat described in the May 2023 National Threat Advisory System (NTAS) bulletin. Over the past year, both domestic violence extremists (DVEs) and homegrown violent extremists (HVEs), who unlike DVEs are inspired by foreign actors, have engaged in violence in reaction to sociopolitical events. These actors are likely to continue to be inspired and motivated by a mix of conspiracy theories; personalized grievances; and enduring racial, ethnic, religious, and anti-government ideologies often shared online.

Since January 2022, DVEs have conducted three fatal attacks in the US Homeland (resulting in 21 deaths), and multiple non-lethal attacks. US law enforcement has disrupted over a half dozen other DVE plots during the same period. Collectively, these incidents focused on a variety of targets, including law enforcement, government, faith-based organizations, retail locations, ethnic and religious minorities, healthcare infrastructure, transportation, and the energy sector.

While DVEs will likely continue to use accessible, easy-to-use weapons for attacks, they also will leverage online platforms and encrypted communications applications to share novel tactics and techniques. Collaboration among violent extremists online is likely to grow as they strive to spread their views, recruit followers, and inspire attacks.

### International terrorism

Foreign terrorist groups, including al-Qa'ida and ISIS, are seeking to rebuild overseas and maintain a worldwide network of supporters that could seek to target the US Homeland. The Department of Homeland Security expects that among state actors, Iran will remain the primary sponsor of terrorism in the US and will continue its efforts to advance plots against individuals in the United States.<sup>4</sup>

## Sabotage

The US authorities do not appear to consider sabotage as a separate, stand-alone threat vector, preferring instead to view it as a tool or method used by nefarious actors and groups.

## Strikes, riots and civil commotion (SRCC)

Recent US history is punctuated with examples of strikes, riots, and civil commotion, the cost of which to both insurers and the insured has been significant (protests sparked by the death of George Floyd in 2020 resulted in \$2.5bn to \$3bn in insured losses).

The triggers for this activity are varied but include the cost of living crisis, a distrust of government or government policy, polarized politics, activism, climate change, and environmental concerns, all of which continue to resonate in the US. For this reason, it is assessed that the threat of SRCC in the US in the short to medium term is, and is likely to remain, real and contemporary.



## Political violence (PV)

The US has a long history of political violence and the US presidential elections of 2016 and 2020 both experienced incidents of such political violence, albeit calm has ensued from the 2024 result. Political polarization, stochastic tools (discussed below), and politicized radicals were always likely to impact the presidential election, touched on elsewhere in this report. There were very few, if any, national (US) or international commentators who did not see political violence as at least some part of the landscape of this year's election; assassination attempts on President Trump bear witness to the accuracy of this sentiment.

## Additional complexity

Additional complexity is added to this already challenging threat landscape by the following dynamics:

### **Stochastic propaganda**

Stochastic propaganda is the public demonization of a person or group to influence perception in a way that is statistically probable but whose specifics cannot be predicted.

Stochastic terrorism is the public demonization of a person or group resulting in the incitement of a violent act which is statistically probable but whose specifics cannot be predicted.

In liberal democracies, freedom of speech and freedom of expression are both enshrined in law and deeply engrained in the DNA of citizens.

These freedoms make the use of stochastic propaganda (and by extension stochastic terrorism) particularly effective because the rhetoric they use is often viewed as 'protected speech'<sup>15</sup> and so is seldom, if ever, sanctioned. For this reason, when employed in environments and amongst people that, for the most part, behave predictably (or at least within tolerances), the impact of these tools can be profound. This is especially true if an act can be spun in such a way that original orators benefit from subsequent effects.

For these reasons, stochastic propaganda is now widely used by more extreme political figures in the US.

### **Pernicious polarization**

Polarization is the extent to which the electorate dislikes or distrusts those from other parties. In the US affective political polarization falls into two broad camps:

- polarization over issues,
- polarization over emotions.

Recent analysis by the International Crisis Group (ICG)<sup>6</sup> identifies that while affective political polarization in the US does exist Americans are not as ideologically polarized as the media would suggest. The same analysis identifies that US voters don't disagree nearly as much as is reported. Overlap of political beliefs among mainstream voters on key issues such as abortion, immigration, and gun control is therefore significant.

Where a clear split does exist is between politicians, who the ICG identified as 'extremely ideologically polarized'. In the US this is now a significant area of friction due to so many congressional seats being considered safe as states generally vote the same way - Democrat or Republican, time after time - broadly the case in 2024 too.

Most political activity at state level occurs around the primaries, during which voters select a candidate to represent a particular party at district and state level.

Therefore, the need to energize voters, or to differentiate a candidate strongly from an opponent, means parties seek to identify, and then exploit levers with real voter resonance.

Increasingly, this lever has become an emotional one with the result that US politicians at state level often now actively pursue a polarizing agenda in order to differentiate themselves from their rivals. This activity, described as 'pernicious polarization',<sup>7</sup> has proved to be an effective tool for energizing voters in America's torpid state election system.

This is important because this type of polarization resonates particularly strongly at the fringes where people are most politicized and most politically engaged. It is also where perceptions of 'the other side' are strongest and where recourse to extremes has proven to be most likely. It is now thought that this type of polarization lay behind much of the political violence which marred the 2020 US election.

‘ US politicians at state level often now actively pursue a polarizing agenda in order to differentiate themselves from their rivals. ’

**Clutter and noise**

The impact of social media, particularly secure social media such as ‘Telegram’, on the malicious risk landscape has been significant. Users of these systems point to the obvious benefits they offer to opposition political actors in places like Syria and Myanmar.

However, those with malign intent offer a variety of counterpoints to the potential positive benefits of these platforms, such as:

1. The anonymity social media offers users is well documented. As the threat from malicious actors evolves the opportunities offered to intimidate, threaten or coerce, or to incite such activities in others while maintaining anonymity should not be underestimated.
2. Hiding in this 'noise' is simple and unless law enforcement agencies are alert to particular users or have access to the strategic resources necessary to identify individuals in such noise, malicious users often remain undetected.

Throughout history the ability to de-centralize and firewall networks has been key to the success of revolutionaries, insurrectionists, and terrorists world-wide. By engineering cut-outs between groups in a network, members can make it far more difficult for national authorities to roll up entire organizations if a single cell is compromised. Communicating between groups in such a construct was always a significant challenge and often it was the compromise of messages or messengers which led to discovery and sanction. The advent of social media has made messaging more secure and the imposition of cut-outs easier to engineer. With encryption and cyber street-craft enhancing the protection already offered by social media, even governments with the technical capability of the US are now finding it difficult to understand and manage the totality of the technical threat of such systems and groups pose.

3. The popularity of social media in the US is significant, with Facebook, Instagram and TikTok being the most influential:<sup>8</sup>



**72.5%**

of the total US population (246 million people) have social network accounts.

Social Network	Monthly Users Active in the US (in millions)
Facebook	177.5
Instagram	138.5
TikTok	107.8
Snapchat	90.5
Pinterest	86.8
X (Twitter)	50.5



# Emerging Trends

## Internationalization

Analysis of the most up-to-date Global Organized Crime Index (GOCI)<sup>9</sup> identifies that international criminal trade and the impact of international criminal actors are significant and growing dynamics in the malicious risk landscape of the US

The same report articulates the risk to the US from international criminal actors in the following terms:

"There are tens of thousands of active criminal gangs across the country. Criminal networks and gangs often collaborate with foreign drug trafficking networks and employ high levels of violence to carry out their operations. Foreign criminal groups also have a significant influence on various criminal activities in the US, including drug and human trafficking, cybercrime and election interference".<sup>10</sup>

Given this growth of transnational criminal networks, it is worth assessing how this dynamic could impact the US risk environment and where it could compound other growing threats. Questions to consider might include:

- The extent to which foreign actors are now being engaged by domestic US criminals and terrorists to conduct activity on their behalf within the US in exchange for goods and services;
- Whether this activity will be in keeping with traditional criminal violence in the US, or could they import new and alternative practices, such as more extreme violence;<sup>11</sup>
- The extent to which foreign states are coordinating their activities with domestic US actors as part of a strategy of hybrid or 'grey zone' warfare;
- Whether domestic US terrorists and criminal actors will seek to exploit the networks of their international partners to enhance their own knowledge, deliver training, and build relationships; and
- Whether, in return for the support they provide, international actors can direct US based criminal organizations and steer them into new activities. Human trafficking is a particularly insidious example of this phenomenon and one that increasingly impacts America's wider security landscape.

The OCI articulates the threat to the US from international illegal trade as follows:

"The US arms trafficking market is large and considerable, with the country serving as both a source and destination for difficult-to-purchase firearms, including machine guns. Guns that are trafficked within and across state lines contribute significantly to domestic violence, but the scope of the market is also transnational. Weapons sourced from the US often end up in the hands of armed gangs, drug traffickers and terrorist organizations abroad, sparking controversial debates over the links between arms proliferation, criminal violence and global terrorism [which] in recent years...has reignited the gun control debate and further polarized partisan divides..."<sup>12</sup>

## Politicized radicals

Almost every week since the start of 2024, the Terrorism Research and Analysis Consortium (TRAC) has identified extremist activity in the US. In July 2024, TRAC stated that "Extreme right-wing ideology has been on the rise in the United States [and] this trend is likely to continue"<sup>13</sup>, and in response to the assassination attempts on President Trump, US Law Enforcement Agencies "...remain concerned about the potential for follow-on or retaliatory acts of violence... particularly given that individuals in some online communities have threatened, encouraged, or referenced acts of violence in response to the attempted assassination".<sup>14</sup>

Far-right and far-left extremism is not a new phenomenon in the US. What is noteworthy is the use by these groups of new strategies to enhance both their attractiveness to recruits, and their influence on the political mainstream, most noticeably:

- New tools, including stochastic propaganda, designed to enable messaging right at the edge of the legal threshold;
- Emulating the communication style of strategic actors who employ inflammatory rhetoric as part of mainstream debate and so legitimately push the boundaries of acceptable political behavior; and
- Presenting themselves as de facto militant wings of political parties to allow them to conduct their activities as part of the US political mainstream. The Proud Boys on the right and Antifa affiliates on the left are amongst the most visible proponents of this emerging dynamic. This is despite the 'demobilization of support groups'<sup>15</sup> following The January 6th Capitol Attack and President Trump's apparent attempt to distance himself from those who marched on the Capitol.

All of which have the potential to impact the stability of America's already fragile political landscape.

## Threats vs acts

"Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of people peaceably to assemble, and to petition the Government for a redress of grievances."

– US First Amendment

The International Crisis Group reports that:

- Hate crimes in the US are at their highest level this century, higher even than after 9/11;
- A fifth of locally elected officials in the US were receiving threats every month in 2023;
- 75% of officials in San Diego County reported having received threats and harassment over the same period; and
- Threats are increasingly anonymous, more frequent and uglier, and are now being delivered physically, via social media and by telephone.

It is not yet clear why this should be the case but while the First Amendment in the US remains as strong as it currently is, it will remain extremely difficult to arrest those making threats in the US.

And so with 'acts' demonstrably resulting in prosecution and 'threats' demonstrably not, the trend to threaten and intimidate in order to influence rather than to act is likely to continue. Should this be the case, and with existing protections in place and unlikely to change, nefarious actors are more rather than less likely to explore the boundaries of this provenly effective vector.

## Grey zone conflict

"The term grey zone conflict captures deliberate multidimensional activities by a state actor just below the threshold of aggressive use of military forces. In such conflicts, adversaries employ an integrated suite of national and subnational instruments of power in an ambiguous war to gain specified strategic objectives without crossing the threshold of overt conflict. Adversaries may employ proxy forces to increase the level of military power being used without losing deniability."<sup>16</sup>

Since that piece was written by Frank G. Hoffman for the Heritage Foundation in October 2015, state actors have honed and refined their skills. Grey zone activity now sits firmly on the front lines of the strategic conflict currently underway between the great powers and their allies. Pre-eminent in this conflict are the activities of China and Russia against the US and within this struggle, subtleties are beginning to emerge which differentiate the activities of those involved and therefore signpost, if not attribute responsibility, at least credible attribution.

Russia in many ways was the leading exponent of grey zone conflict for many years and certainly appeared to lead in its use up to the start of this decade. Examples of cyber and social media activity to influence the US Presidential Election in 2016 were the most widely reported example of this strategy. Russia's response to US imposed sanctions following their invasion of Ukraine in 2022 appear to have redoubled Russian efforts to use grey zone methods to exert influence on the US.

China's approach to grey zone conflict in the US appears to have been more subtle than that employed by Russia, but there is now some evidence to suggest that China's grey zone activity in America is significant. Forming a key element of China's 'Three Warfares' (public opinion warfare, psychological warfare, and legal warfare), grey zone activity is now a long-term, strategically resourced tool of the Chinese state.

## Where does this lead?

Deniability lies at the core of grey zone DNA. And by the nature of the of stochastic tools, the anonymity of social media, and the subtlety of threat (rather than act) all play well with deniability.

Targeting cracks in existing national dynamics to achieve affect have long been recognized and employed as tools of influence; pernicious polarization and the politicization of radicals are two contemporary examples of such opportunity.

And allying international organized crime with the existing and expanding networks of US criminals provides both the ways and the means for state actors to conduct deniable nefarious activity within the US.



## Existing Mitigation Strategies

The insurance industry has worked hard to keep pace with the evolution of malicious risk and to develop and offer products capable of protecting the insured against a wide spectrum of malicious perils. In broad terms, these offerings provide effective cover for both traditional terrorism exposure and several hybrid threats (political violence, active assailant, SRCC). What has yet to be explored is the extent to which these products will protect the insured in the event of a non-linear, complex or systemic issue involving multiple perils and which falls outside modelled scenarios.

This is important; by continuing to refer to coverage as 'protection' while constraining this protection to pre-defined paradigms (including mandated triggers) how much protection is actually being offered in a world of complex and emerging threats?

In a sector already prone to coverage complexity, insurance policies can contain various forms of malicious risk coverage. In addition, the market is not uniform in its approach. Where some policies have absolute exclusion / exception, others do not, and policies may have an extension in certain instances. But even where an extension exists, the language can be ambiguous in its definition. Time and scale elements may be used by a carrier to argue for non-coverage of a particular incident.

Issues are now spreading further left along the spectrum, i.e. pre-incident, to threaten the insured in a meaningful way as early as the 'evolution phase' of a developing threat. With this in mind, how responsive is the market likely to be in a landscape that has already outgrown much of its existing wording? Where stochastic (unattributable) activity is now a mainstream strategy; and where soft effects (including cancel culture and being cancelled) are now as impactful as direct action.

Should the insurance industry re-define 'protection' as a result? What now should be the principles which guide the industry's instinct and behavior to protect? And where on the spectrum of risk should protection now begin?





## Conclusion

The insurance products offered in the market today typically deliver a protective wrapper to clients which is perceived to be fit for purpose to help mitigate the prevailing threats.

The reality of malicious actors is that they seldom stand-still and often it is their acts and methods which drive the evolution of threat (and therefore threat mitigation) rather than those charged with providing protection solutions, including risk transfer. Silos of isolated risk and insurance policies to address these, are frequently found in the market.

Within this environment, organisations which lack the agility or the insight and intelligence to keep pace with adversaries end-up responding to threats rather than anticipating them. As has been shown throughout history, being on the back foot is seldom optimum when complex crises hit.

So, in a sea of metaphorical super-tankers, perhaps it is the small, fast, agile market players which are best placed to support those exposed to ever-evolving malicious risks. Do they have the drive and dynamism, aligned with this presumed agility, to offer the required options in a dynamic risk environment when people, assets, and the bottom-line must be protected?



# About Samphire Advisory

This report has been researched and produced by Samphire Advisory, our in-house team of malicious risk consultants. The multi-disciplined team focuses on mitigation, threat intelligence, and risk analysis. Our advisors are trusted in some of the world's most demanding sectors, providing the strategic insight, operational resilience, and tactical support necessary to develop awareness, mitigate risk, and protect the bottom line.

The Samphire Advisory team allows us to provide our partners and clients with greater understanding and the ability to mitigate malicious and hostile risk. Our insurance products allow them to transfer risk if required, positioning us as an expert provider of what is needed to protect people and companies from 'bad people doing bad things'.

This capability also enables us to fuse the deep understanding and significant knowledge of our underwriters with the insight and experience of our consultants. This nexus helps us to develop market leading products at the forefront of malicious risk mitigation, and to operate at the leading edge of insurance innovation.

## References

1. <https://www.genre.com/content/dam/generalreinsuranceprogram/documents/pmint20-4-en.pdf>
2. <https://www.chubb.com/uk-en/business/products/terrorism-insurance/political-violence-terrorism-insurance.html>
3. <https://www.munichre.com/us-non-life/en/solutions/specialty-insurance/terrorism-political-violence-coverage.html>
4. [https://www.dhs.gov/sites/default/files/2023-09/23\\_0913\\_ia\\_23-333-ia\\_u\\_homeland-threat-assessment-2024\\_508C\\_V6\\_13Sep23.pdf](https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf)
5. 'Stochastic Terrorism, Speech Incantations and Federal Tax Exemption', Darryll K. Jones, New Mexico Law Review, Volume 54 Issue 1 Winter, dated Winter 2024
6. [www.crisisgroup.org/united-states/polarisation-political-violence-and-us-elections](http://www.crisisgroup.org/united-states/polarisation-political-violence-and-us-elections)
7. Jenefer McCoy and Marat Summer quoted in 'Polarisation, Political Violence and the US Elections', the ICG dated 19 April 2024
8. <https://backlinko.com/social-media-users>
9. <https://ocindex.net/report/2023/0-3-contents.html>
10. [https://ocindex.net/country/united\\_states](https://ocindex.net/country/united_states)
11. The scale and scope of criminal violence in Europe increased significantly following the fall of the Berlin Wall as criminal actors from eastern Europe moved west bringing patterns of behaviour (and an appetite for violence) well in excess of western European criminal norms at that time.
12. [https://ocindex.net/country/united\\_states](https://ocindex.net/country/united_states)
13. TRACWatch - Weekly Analyst Briefing, Weekly Analysts Review, 11 July 2024 (<https://trackingterrorism.org/analysts-briefing/>)
14. <https://edition.cnn.com/2024/08/08/politics/democratic-convention-target-extremists/index.html>
15. 'Polarisation, Political Violence and the US Elections', the ICG dated 19 April 2024
16. [www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protected-gray](http://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protected-gray)



## About Samphire Risk

Samphire Risk was formed in 2021 and is a world-leading independent Managing General Agent (MGA) focused on insuring people and companies against hostile and malicious risks. Through an expert team and exceptional technology, Samphire aims to create world-class products that insure against extortive crime, hostage-taking and kidnap; terrorism in all its guises; travel into, and within, insecure countries and locations.

To find out more about Samphire please visit our website [www.samphirerisk.com](http://www.samphirerisk.com) or follow us on LinkedIn.

Samphire and Samphire Risk are trading names of Samphire Services Limited which is an appointed representative of Davies MGA Services Limited, a company authorised and regulated by the Financial Conduct Authority under firm reference number 597301 to carry on insurance distribution activities. Samphire Services Limited is registered in England and Wales number 13421262. Registered Office: 1-3 Leadenhall Market, London, EC3V 1LR



January 2025